Computing Sector has created an overall IT Service Continuity Management Plan that covers the key areas that each individual plan would rely upon in a continuity situation such as command center information, vital records, personnel information. The purpose of this document is to describe the key information needed to recover this service in a business continuity situation once a decision to invoke has been made, and then to manage the business return to normal operation once the service disruption has been resolved.

Scope

Service Area: Central Authentication

Service Offerings: FNAL.GOV Kerberos Realm (Kerberos)

FERMI Windows Domain (Fermi)

KCA Service (KCA)

LDAP Service (LDAP)

Service Areas that depend on this service: Unknown

Recovery Objectives

Recovery Time Objective (RTO) < 4 Hours

Recovery Point Objective (RPO) > 4 hours

Recovery Team

In this section describe the other services, roles, and responsibly required for recovering this service.

Service/Role/Function	**Responsibility**	**Dependencies**	**Expected Response Time**
Kerberos Administrator	Kerberos	Network, Power, Facilities	<4 hours
Active Directory Administrator	Fermi, LDAP	Network, Power, Facilities	<4 hours
Windows Administrator	KCA	Network, Power, Facilities	<4 hours
External Service Provider –Microsoft	Fermi, LDAP	Fermi, LDAP	< 4 hour
External Service Provider – Secure Endpoints	Kerberos, KCA	Kerberos , KCA, Fermi	< 4 hours

Recovery Strategy

Failover to redundant systems, restore (onto new hardware), rebuild from scratch (on new hardware)

Strategy for initial recovery

Initial recovery is to rely on failover to redundant systems located on site.

Overall recovery strategy

Datacenter Outages

Single Datacenter Outage – Services continue normal function. Depending on the Datacenter the A record for the LDAP service, services.fnal.gov, may need to be updated by Network Services to remove the LDAP server that is offline from the A record.

Two Datacenter Outage – Depending on which datacenters suffer from the outage the LDAP Service and the KCA Service could be offline. In addition the A record for the LDAP service, services.fnal.gov, may need to be updated by Network Services to remove the LDAP server that is offline from the A record. The Kerberos service and the Fermi Windows Domain will continue to function.

Total Loss (Infrastructure / Data) – Rebuild from scratch

High availability fail-over

Authentication systems are hosted in multiple computer rooms/buildings at Fermilab. Compete failure of the Kerberos and Fermi Windows Domain services would require the computer rooms in WH8, FCC2, FCC3, AD Controls, and D0 to be offline. Complete failure of the LDAP Service and KCA Service would require the computer rooms located on WH8 and FCC2 to be offline.

Recover at another site or multiple sites

A "Disaster Recovery" site exists for the Kerberos and Fermi Windows Domain services exist at Argonne National Laboratory for Business Service Applications. It is not intended for general purpose use.

Build from scratch

Kerberos: Requires specialized hardware no longer available from the vendor. Assuming hardware was available the service could be available in 24 hours if data can be recovered. A complete rebuild from scratch would require an operational CNAS service and would take longer than 24 hours.

Fermi: Assuming hardware was available and the backups can be recovered the service could be available in less than 24 hours. A complete rebuild from scratch would require an operational CNAS service and would take longer than 24 hours.

KCA: Requires specialized hardware that is not available over the counter. Assuming that this hardware had to be ordered it would be greater than 72 hours to recover.

LDAP: Assuming hardware was available and the backups can be recovered the service could be available in less than 24 hours. A complete rebuild from scratch would require an operational Fermi Windows Domain and would take longer than 24 hours.

Recovery Scenarios

Building not accessible (Data Center Available)

- If only a single datacenter impacted verify service is functional
- Systems are set to boot when power is applied.
- Access systems once network is available and verify operations
- Perform physical inspection once building is accessible

Data Center Failure (Building Accessible)

- If only a single datacenter impacted verify service is functional
- Perform physical inspection of infrastructure
- Systems are set to boot when power is applied.
- Access systems once network is available and verify operations

Building not accessible and Data Center Failure

- If only a single datacenter impacted verify service is functional
- Systems are set to boot when power is applied.
- Access systems once network is available and verify operations
- Perform physical inspection once building is accessible

Critical recovery team not available

- Local expertise is sufficient to restore service in the majority of situations.
- Microsoft Premier Support is guaranteed response
- Kerberos administrative access is single point of failure if Secure Endpoints is not available

Return to Operations

Kerberos

- Verify account lifecycle
- Verify account management
- Verify replication
- Verify account usage

Fermi

- Verify account lifecycle
- Verify account management

- Verify replication
- Verify account usage

KCA

- Verify certificate issuance

LDAP

- Verify account lifecycle
- Verify account management
- Verify replication
- Verify account usage

Document Change Log

Version	Date	Author(s)	Change Summary
1	8/7/2012	A. Lilianstrom	Initial version
1.1	3/14/2013	A. Lilianstrom	Update for LDAP Service